Port Specification

In Nmap (Network Mapper), a port specification is a way to define which network ports should be scanned on a target system. Nmap is a powerful open-source tool used for network discovery and security auditing. It allows users to discover hosts and services on a computer network, highlighting open ports and other information that can be useful for assessing the security of a network.

Port specifications in Nmap can be quite flexible, allowing users to specify individual ports, ranges of ports, or even use special keywords to represent common groups of ports. Here are some examples:

1. Individual Port:

```
nmap -p 80 target.com
```

2. Port Range:

```
nmap -p 1-100 target.com
```

3. Combination of Individual Ports and Ranges:

```
nmap -p 80,443,8000-8100 target.com
```

4. Top Ports (Nmap will scan the most common 1,000 ports):

```
nmap --top-ports 1000 target.com
```

5. Port Exclusion:

```
nmap -p 1-100 --exclude-ports 20,80 target.com
```

6. Port scan all ports:

```
nmap -p- target.com
```

7. Port scan from service name:

```
nmap -p http,ssh,dns,target.com
```

8. Port scan multiple TCP and UDP ports:

```
nmap -p U:53,T:21-25,80 192.168.1.1
```

9. Fast port scan (100 ports):

   The -F option in Nmap stands for "Fast mode," and it is used to perform a fast scan by only scanning the most common 100 ports. If you want to use the -F option, the correct syntax would be:

```
nmap -F 192.168.1.1
```